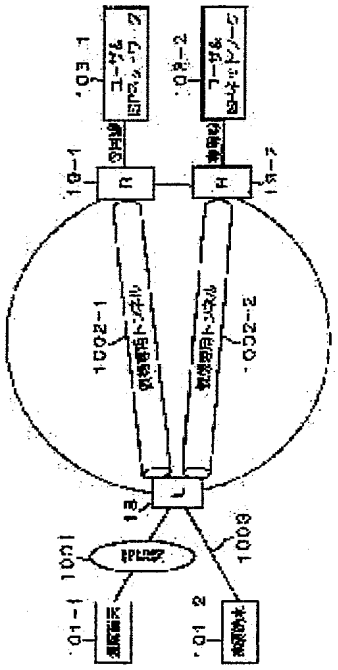
Ref. 1 (Machine Translation)

Jpn. Pat. Appln. KOKAI Publication 2002-135313

SP Number : A0006P3167

(English Documments Translated by Translation Software)

# (54) COMMUNICATION SYSTEM AND COMMUNICATION METHOD



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication system that can secure the security and simplifies the communication processing so as to attain a high data communication processing speed.

SOLUTION: An IP network remote access controller 18 discriminates an access destination code designated by remote terminals 101-1 and 101-2 of users and sets a path of a virtual dedicated tunnel 1002-1 or 1002-2 with respect to a corresponding IP network terminator 19-1 or 19-2. Furthermore, the IP network remote access controller 18 decapsulates user data and makes IP packet communication between the corresponding IP network terminators 19-1 and 19-2 via the virtual dedicated tunnel. The corresponding IP network terminators 19-1 and 19-2 eliminate a capsule header and transmit the result to a user and ISP network 103-1 or 103-2 as an IP packet.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## CLAIMS

---

[Claim(s)]

[Claim 1]A communications system which is provided with the following, and said IP network remote attachment control means is encapsulating an user datum transmitted and received between IP network network terminations corresponding to a connection destination specified from said remote terminal side, and is characterized by building a tunnel only for imagination.

An IP network remote attachment control means to which it is a communications system which connects with a connection destination network via an IP network from a remote terminal, and transmits and receives data, and is allocated on said IP network, and direct continuation of said remote terminal is carried out via a public network.

An IP network network termination means which is allocated on said IP network and connected to said connection destination network.

[Claim 2]The communications system comprising according to claim 1:

Said said IP network remote attachment control means, A connection destination distribution means to identify connection destination numerals specified from said remote terminal side, to build a tunnel only for imagination between an IP network network termination and self corresponding to a connection destination shown with these connection destination numerals, and to distribute data from the remote terminal side to a connection destination network.

An encapsulation means to encapsulate data in order to transmit data to a tunnel only for imagination built by said connection destination distribution means.

[Claim 3]It connects with a connection destination network via an IP network from a

remote terminal, A correspondence procedure which is a correspondence procedure which transmits and receives data and is characterized by building a tunnel only for imagination by encapsulating an user datum transmitted and received between an IP network remote attachment control device on said IP network, and a network termination for IP networks.

[Claim 4]The correspondence procedure according to claim 3 specifying a network termination for IP networks corresponding to a connection destination network which should be carried out a connection destination based on a connection destination identification signal specified from said remote terminal when connecting it with said connection destination network via an IP network from said remote terminal.

---

[Translation done.]

* NOTICES *



1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the communications system and correspondence procedure which connect with a connection destination network via an

IP network from a remote terminal, and transmit and receive data.

[0002]

[Description of the Prior Art]Conventionally, as shown in drawing 5, via the telephone network which comprises a transit exchange, The remote terminal 101-1, 101-2, and the user &ISP (Internet Service Provider) network 103-1 and 103-2, It connects by user & ISP networks 103-1, the contact (entrance) 14-1 by the side of 103-2, and 14-2, and the communications system which transmits and receives data is known.

[0003]In this case, in order to communicate between the remote terminal 101-1, 101-2, and user & ISP networks 103-1 and 103-2, securing security, . [ whether between the contact 14-1, 14-2, and user & ISP networks 103-1 and 103-2, as shown in drawing 5, the phi wall device 16-1 which prevents an unauthorized entry, and 16-2 are installed, in order to prevent the attack from the network outside, and ] The contact 14-1 and 14-2 the very thing were equipped with the firewall function, further, by the communication function of 101-2, the IP packet was enciphered, it encapsulated, and the remote terminal side 101-1 had transmitted and received.

[0004]

[Problem(s) to be Solved by the Invention]As mentioned above, in the conventional correspondence procedure, the firewall device 16-1 and management of 16-2 were needed, and, as for the remote terminal side 101-1, load was applied also to 101-2 for encryption of an IP packet, and encapsulation processing, and there was a problem that communications processing became complicated.

[0005]While being made in view of the situation mentioned above and being able to secure security, this invention simplifies communications processing and an object of an invention is to provide the communications system and correspondence procedure which can attain improvement in the speed of data communication processing speed.

[0006]

[Means for Solving the Problem]In order to solve a problem mentioned above, in the invention according to claim 1. It is a communications system which connects with a connection destination network via an IP network from a remote terminal, and transmits and receives data, An IP network remote attachment control means to which it is

allocated on said IP network and direct continuation of said remote terminal is carried out via a public network, It is allocated on said IP network, provide an IP network network termination means connected to said connection destination network, and said IP network remote attachment control means, A tunnel only for imagination is built by encapsulating an user datum transmitted and received between IP network network terminations corresponding to a connection destination specified from said remote terminal side.

[0007]This invention is characterized by that the communications system according to claim 1 comprises the following by the invention according to claim 2 again.

Said said IP network remote attachment control means, A connection destination distribution means to identify connection destination numerals specified from said remote terminal side, to build a tunnel only for imagination between an IP network network termination and self corresponding to a connection destination shown with these connection destination numerals, and to distribute data from the remote terminal side to a connection destination network.

An encapsulation means to encapsulate data in order to transmit data to a tunnel only for imagination built by said connection destination distribution means.

[0008]In order to solve a problem mentioned above, in the invention according to claim 3. It connects with a connection destination network via an IP network from a remote terminal, A tunnel only for imagination is built by being a correspondence procedure which transmits and receives data and encapsulating an user datum transmitted and received between an IP network remote attachment control device on said IP network, and a network termination for IP networks.

[0009]In the correspondence procedure according to claim 3 by the invention according to claim 4, When connecting it with said connection destination network via an IP network from said remote terminal, based on a connection destination identification signal specified from said remote terminal, a network termination for IP networks corresponding to a connection destination network which should be carried out a connection destination is specified.

[0010]In this invention, it is allocated on an IP network and said remote terminal by an IP network remote attachment control means by which direct continuation is carried out via a public network. A tunnel only for imagination is built by encapsulating an user datum transmitted and received between IP network network terminations corresponding to a connection destination specified from said remote terminal side. Therefore, it becomes possible to secure security, and to transmit and receive data being unconscious of a physical network.

[0011]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described using a drawing.

A. The lineblock diagram 1 of an embodiment is a block diagram showing the system configuration of the whole by the embodiment of this invention. The same numerals are attached to the portion corresponding to drawing 5, and explanation is omitted. In drawing 1, the IP network remote attachment control device 18, It is controlled to according to specification of the connection destination from the remote terminal 101-1 side and 101-2 side, the tunnel 1002-1 only for imagination and 1002-2 are built to which of user & ISP networks 103-1 and 103-2, and data is distributed. The IP network remote attachment control device 18 encapsulates an user datum, in order to transmit data to the above-mentioned tunnel only for imagination, and it performs IP packet communication between the IP network network termination 19-1 and 19-2.

[0012]The IP network network termination 19-1 and 19-2 are the closed network terminating sets of the tunnel only for imagination of the IP network for connecting with user & ISP networks 103-1 and the ISP networks of 103-2. The IP network network termination 19-1 and 19-2, It has an interface which connects a course with the tunnel 1002-1 only for imagination, and the tunnel 1002-2 only for imagination, The received data is transmitted to user & ISP networks 103-1 or 103-2 after building the tunnel only for imagination with the IP network remote attachment control device 18 (closed network). In that case, the IP network network termination 19-1 and 19-2 remove a capsule header from the data encapsulated by the above-mentioned IP network remote attachment control device 18, and transmit to user & ISP networks 103-1 and 103-2 as

an IP packet.

[0013]As for the remote terminal 101-1 of the end user, the remote terminal 101-2 is connected with the IP network remote attachment control device 18 by the dedicated line 1003 via the telephone network 1001. The remote terminal 101-1 and 101-2 control between the IP network remote attachment control device 18, the IP network network termination 19-1, and 19-2 respectively to secure and carry out the data communications of user & ISP networks 103-1, and 103-1 and security.

[0014]Next, drawing 2 is a block diagram showing the composition of the IP network remote attachment control device 18. In drawing 2, the IP network remote attachment control device 18 is provided with the connection destination distribution functional module 21 and the encapsulation functional module 22. The connection destination distribution functional module 21 controls whether the data received through the telephone network and the dedicated line is connected to which of user & ISP networks 103-1 and 103-1, and it transmits. This connection destination distribution functional module 21 has the connection destination course selection table 210 shown in drawing 3 (a).

[0015]The above-mentioned connection destination distribution functional module 21 is specified by remote terminal [ of a user ] 101-1 and 101-2 side, . Distinguish the transmitted connection destination numerals and are stored in the connection destination course selection table 210. Either IP address of the IP network network termination 19-1 used as the exit of the tunnel only for imagination matched with the ISP identification signal and the IP network network termination 19-2 is chosen, and routing of the tunnel 1002-1 only for imagination or the tunnel 1002-2 only for imagination is performed. Multidata input is possible for the above-mentioned connection destination course selection table 210.

[0016]The encapsulation functional module 22 encapsulates an user datum, in order to transmit data to the tunnel only for imagination by which routing was carried out with the above-mentioned connection destination distribution functional module 21. The encapsulated user datum is transmitted as IP packet data 220 which have a frame structure shown in drawing 3 (b). This encapsulation functional module 22 makes

between the IP network remote attachment control device 18, the IP network network termination 19-1, and 19-2 tunnel above-mentioned IP packet data 220, and performs IP packet communication. Since the encapsulated data 220, i.e., IP packet data, is transmitted as an IP packet at this time, it can communicate without receiving restrictions of a physical net.

[0017]B. Explain operation of an embodiment, next operation of this whole embodiment in detail. It is specified by remote terminal [ of a user ] 101-1 and 101-2 side in the connection destination distribution functional module 21, Distinguish the transmitted connection destination numerals and the connection destination course selection table 210 is referred to, The IP address of the exit of the tunnel corresponding to an ISP identification signal is chosen, and routing of the tunnel only for imagination (1002-1 or 1002-2) to the IP network network termination (19-1 or 19-2) of this IP address is performed.

[0018]An user datum is encapsulated in order that the encapsulation functional module 22 may transmit data to the tunnel only for imagination (1002-1 or 1002-2) by which routing was carried out with the above-mentioned connection destination distribution functional module 21, IP packet communication is performed between the IP network remote attachment control device 18, the IP network network termination 19-1, and 19-2.

[0019]In the IP network network termination 19-1 and 19-2, the received data is transmitted to user & ISP networks 103-1 or 103-2 after building the tunnel only for imagination with the IP network remote attachment control device 18 (closed network). At this time, the capsule header shown in drawing 3 (b) is removed, and an user datum is transmitted as an IP packet.

[0020]In the embodiment mentioned above, user & ISP networks 103-1 of a connection destination and 103-2 can be chosen from the remote terminal 101-1 and 101-2 by user initiative, After connection, being unconscious of a physical net, security can be secured, and data can be transmitted only by using the tunnel art which encapsulates an IP packet and received.

[0021]C. Describe other embodiments, next other embodiments of this invention.

Drawing 4 is a block diagram showing the system configuration at the time of connecting with two or more user & ISP networks via an IP network depended on other carried-out types of this invention. The same numerals are attached to the portion corresponding to drawing 1, and explanation is omitted. The IP network network termination 19-1 - 19-n are connected to respectively corresponding user & ISP networks 103-1 - 103-n.

[0022]The IP network remote attachment control device 28, It is equivalent to the IP network remote attachment control device 18 shown in drawing 1, and User & ISP networks 103-1 - the connection destination numerals of 103-n, It has the connection destination course selection table (graphic display abbreviation) where the IP address of the IP network network termination 19-1 used as the exit of the tunnel only for imagination - 19-n was matched.

[0023]. This corresponds to either two or more user & ISP networks 103-1 specified as two or more user & ISP networks 103-1 - 103-n by the remote terminal [ of a user ] 101-1 - 101-n side - 103-n. The tunnel only for imagination (closed network: either of the 1002-1 - 1002-n) is built, security is secured, and IP packet communication is performed.

[0024]Although the closed network mentioned above is a logical virtual private network, The closed network which uses circuits, such as a dedicated line physical besides, a Frame Relay, and ATM, is piled up, Even when between the IP network remote attachment control device 18 (or 28), the IP network network termination 19-1, and 19-2 (or 19-1 - 19-n) is connected and built, a closed network can be realized similarly.

[0025]It may be made to realize the function of the IP network remote attachment control device 18 (or 28) by executing the program memorized by the storage parts store which is not illustrated. In this case, a storage parts store shall be constituted by nonvolatile memory, such as a hard disk drive, optical-magnetic disc equipment, and a flash memory, volatile memories like RAM (Random Access Memory), or such combination. With the above-mentioned storage parts store, the thing holding a fixed time program is also included like the volatile memory (RAM) inside the computer system used as a server when a program is transmitted via communication lines, such as networks, such as the Internet, and a telephone line, or a client.

[0026]The above-mentioned program may be transmitted to other computer systems via a transmission medium from the computer system which stored this program in memory storage etc. by the transmitted wave in a transmission medium. Here, the "transmission medium" which transmits a program says the thing of a medium which has the function to transmit information like communication lines, such as networks, such as the Internet, and a telephone line. The above-mentioned program may be for realizing a part of processing mentioned above. They may be what can realize processing mentioned above in combination with the program already recorded on the IP network remote attachment control device 18 (or 28), and what is called a patch file (difference program).

[0027]As mentioned above, although the embodiment of this invention has been explained in full detail with reference to drawings, concrete composition is not restricted to the above-mentioned embodiment, and the design etc. of the range which does not deviate from the gist of this invention are included.

[0028]

[Effect of the Invention]As explained above, according to this invention, a virtual private network (closed network) can be built in an IP network only with the tunnel art of making an IP packet encapsulating, and the advantage that communication which secured security to the attack from the outside can be performed is acquired. Introduction of structure, such as introduction of the gateway unit which prevents an unauthorized entry, and encryption, becomes unnecessary by this, facility cost can be reduced, and the advantage that a cost merit can be planned is acquired.

---

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram showing the system configuration of the whole by the embodiment of this invention.

[Drawing 2]It is a block diagram showing the composition of an IP network remote attachment control device.

[Drawing 3]It is a key map showing the packet composition of the user datum (IP packet data) by which the connection destination course selection table was constituted and encapsulated.

[Drawing 4]It is a block diagram showing the system configuration at the time of connecting with two or more user & ISP networks via an IP network depended on other carried-out types of this invention.

[Drawing 5]It is a block diagram showing the conventional system configuration.

[Description of Notations]

18, 28 IP-network remote attachment control device (IP network remote attachment control means)

19-1 - a 19-n IP network network termination (IP network network termination means)

21 Connection destination distribution functional module (connection destination distribution means)

22 Encapsulation functional module (encapsulation means)

101-1-101-n Remote terminal

103-1-103-n User & ISP networks

210 Connection destination course selection table

1001 Telephone network

---

[Translation done.]

* NOTICES *

**JPO and INPIT are not responsible for any damages caused by the use of this translation.**

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

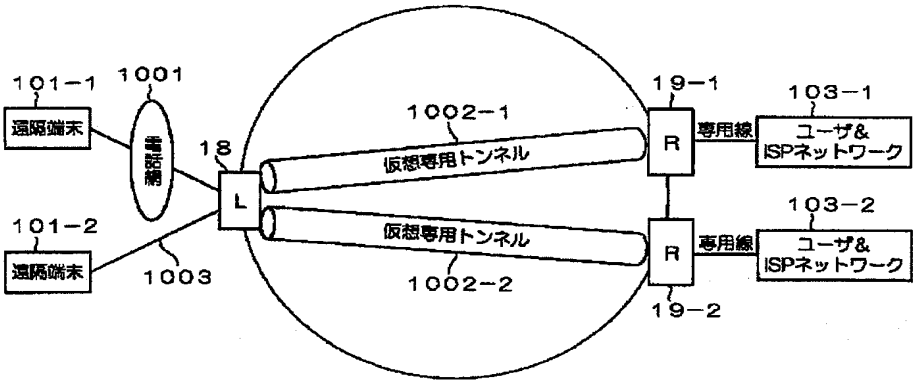
3.In the drawings, any words are not translated.

---

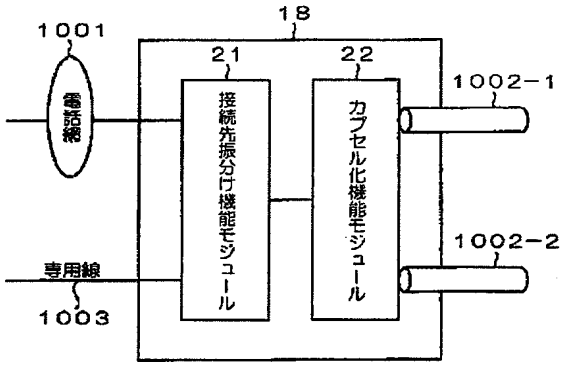
## DRAWINGS

---

[Drawing 1]




[Drawing 2]




[Drawing 3]

(a)

210

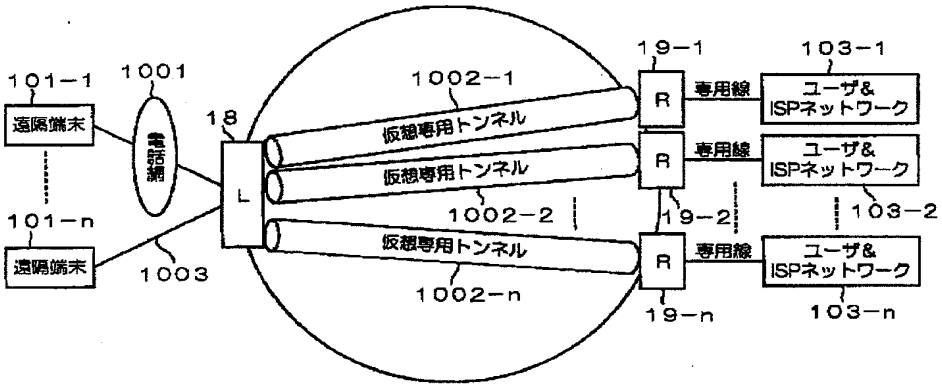
| ISP識別符号 | トンネル出口(R)のIPアドレス |
|---|---|
| aaaaaaa | xx.xx.xx.xx |
| bbbbbbb | xx'.xx'.xx'.xx' |

(b)

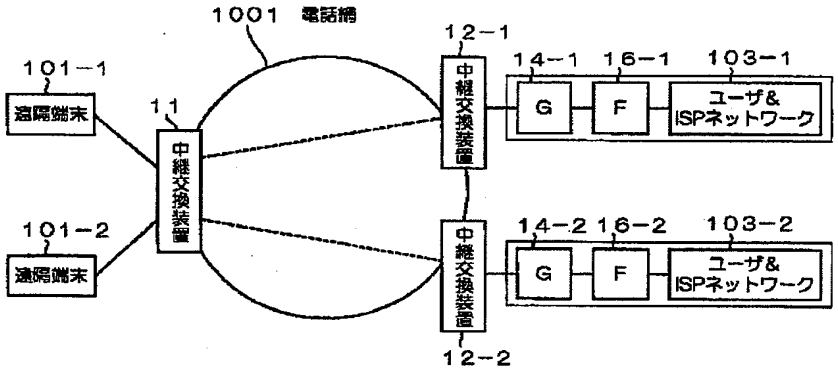
220

| 物理 | IP | カプセルヘッダ | ユーザデータ |
|---|---|---|---|

[Drawing 4]




[Drawing 5]




[Translation done.]

Ref. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－135313
（P2002－135313A）
(43)公開日　平成14年５月10日(2002.5.10)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ　12/56 | | Ｈ０４Ｌ　11/20 | １０２Ａ | ５Ｋ０３０ |
| 12/22 | | | １０２Ｆ | ５Ｋ０３４ |
| 29/04 | | 11/26 | | |
| | | 13/00 | ３０３Ｚ | |

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願2000－325804(P2000－325804)

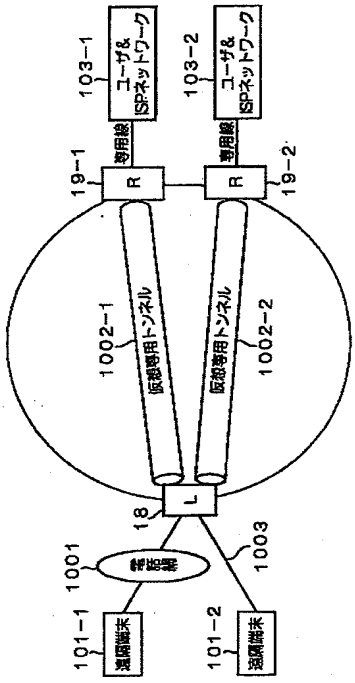
(22)出願日　平成12年10月25日(2000.10.25)

(71)出願人　399040405
東日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号
(72)発明者　川上　弥
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(72)発明者　小池　正仁
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武

最終頁に続く

(54)【発明の名称】　通信システムおよび通信方法

(57)【要約】
【課題】　セキュリティを確保することができるとともに、通信処理を簡素化し、データ通信処理速度の高速化を図る。
【解決手段】　ＩＰネットワーク遠隔接続制御装置１８は、ユーザの遠隔端末１０１－１、１０１－２側によって指定された接続先符号を判別し、対応するＩＰネットワーク網終端装置１９－１または１９－２に対する仮想専用トンネル１００２－１または１００２－２の経路設定を行う。また、ＩＰネットワーク遠隔接続制御装置１８は、ユーザデータをカプセル化し、仮想専用トンネルを介してＩＰネットワーク網終端装置１９－１、１９－２との間でＩＰパケット通信を行う。ＩＰネットワーク網終端装置１９－１、１９－２は、カプセルヘッダを取り除き、ＩＰパケットとしてユーザ＆ＩＳＰネットワーク１０３－１または１０３－２に送信する。



1

【特許請求の範囲】

【請求項１】　遠隔端末からＩＰネットワーク経由で接続先ネットワークに接続してデータを送受信する通信システムであって、

前記ＩＰネットワーク上に配設され、前記遠隔端末が公衆回線網を介してもしくは直接接続されるＩＰネットワーク遠隔接続制御手段と、

前記ＩＰネットワーク上に配設され、前記接続先ネットワークに接続されるＩＰネットワーク網終端手段とを具備し、

前記ＩＰネットワーク遠隔接続制御手段は、前記遠隔端末側から指定される接続先に対応するＩＰネットワーク網終端装置との間で送受信するユーザデータをカプセル化することで、仮想専用トンネルを構築することを特徴とする通信システム。

【請求項２】　前記前記ＩＰネットワーク遠隔接続制御手段は、

前記遠隔端末側から指定される接続先符号を識別し、該接続先符号により示される接続先に対応するＩＰネットワーク網終端装置と自身との間に仮想専用トンネルを構築し、遠隔端末側からのデータを接続先ネットワークに振り分ける接続先振分け手段と、

前記接続先振分け手段により構築された仮想専用トンネルにデータを送信するためにデータをカプセル化するカプセル化手段とを具備することを特徴とする請求項１記載の通信システム。

【請求項３】　遠隔端末からＩＰネットワーク経由で接続先ネットワークに接続し、データを送受信する通信方法であって、

前記ＩＰネットワーク上のＩＰネットワーク遠隔接続制御装置とＩＰネットワーク用網終端装置との間で送受信するユーザデータをカプセル化することで、仮想専用トンネルを構築することを特徴とする通信方法。

【請求項４】　前記遠隔端末からＩＰネットワーク経由で前記接続先ネットワークに接続する際、前記遠隔端末から指定された接続先識別符号に基づいて、接続先すべき接続先ネットワークに対応するＩＰネットワーク用網終端装置を特定することを特徴とする請求項３記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、遠隔端末からＩＰネットワーク経由で接続先ネットワークに接続してデータを送受信する通信システムおよび通信方法に関する。

【０００２】

【従来の技術】従来より、図５に示すように、中継交換機で構成される電話網を介して、遠隔端末１０１－１、１０１－２とユーザ＆ＩＳＰ（Internet Service Provider）ネットワーク１０３－１、１０３－２とを、ユーザ＆ＩＳＰネットワーク１０３－１、１０３－２側の接

2

続装置（入り口）１４－１、１４－２によって接続し、データの送受信を行う通信システムが知られている。

【０００３】この場合、遠隔端末１０１－１、１０１－２とユーザ＆ＩＳＰネットワーク１０３－１、１０３－２との間で、セキュリティを確保しながら通信するには、ネットワーク外部からの攻撃を防ぐために、図５に示すように、接続装置１４－１、１４－２とユーザ＆ＩＳＰネットワーク１０３－１、１０３－２との間に不正侵入を防止するファイウォール装置１６－１、１６－２を設置するか、接続装置１４－１、１４－２自体にファイアウォール機能を備え、さらに遠隔端末側１０１－１、１０１－２の通信機能によりＩＰパケットを、暗号化、カプセル化して送受信していた。

【０００４】

【発明が解決しようとする課題】上述したように、従来の通信方法では、ファイアウォール装置１６－１、１６－２の管理が必要となり、またＩＰパケットの暗号化、カプセル化処理のために遠隔端末側１０１－１、１０１－２にも負荷がかかり、通信処理が複雑になるという問題があった。

【０００５】この発明は上述した事情に鑑みてなされたもので、セキュリティを確保することができるとともに、通信処理を簡素化し、データ通信処理速度の高速化を図ることができる通信システムおよび通信方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】上述した問題点を解決するために、請求項１記載の発明では、遠隔端末からＩＰネットワーク経由で接続先ネットワークに接続してデータを送受信する通信システムであって、前記ＩＰネットワーク上に配設され、前記遠隔端末が公衆回線網を介してもしくは直接接続されるＩＰネットワーク遠隔接続制御手段と、前記ＩＰネットワーク上に配設され、前記接続先ネットワークに接続されるＩＰネットワーク網終端手段とを具備し、前記ＩＰネットワーク遠隔接続制御手段は、前記遠隔端末側から指定される接続先に対応するＩＰネットワーク網終端装置との間で送受信するユーザデータをカプセル化することで、仮想専用トンネルを構築することを特徴とする。

【０００７】また、請求項２記載の発明では、請求項１記載の通信システムにおいて、前記前記ＩＰネットワーク遠隔接続制御手段は、前記遠隔端末側から指定される接続先符号を識別し、該接続先符号により示される接続先に対応するＩＰネットワーク網終端装置と自身との間に仮想専用トンネルを構築し、遠隔端末側からのデータを接続先ネットワークに振り分ける接続先振分け手段と、前記接続先振分け手段により構築された仮想専用トンネルにデータを送信するためにデータをカプセル化するカプセル化手段とを具備することを特徴とする。

【０００８】また、上述した問題点を解決するために、

請求項３記載の発明では、遠隔端末からＩＰネットワーク経由で接続先ネットワークに接続し、データを送受信する通信方法であって、前記ＩＰネットワーク上のＩＰネットワーク遠隔接続制御装置とＩＰネットワーク用網終端装置との間で送受信するユーザデータをカプセル化することで、仮想専用トンネルを構築することを特徴とする。

【０００９】また、請求項４記載の発明では、請求項３記載の通信方法において、前記遠隔端末からＩＰネットワーク経由で前記接続先ネットワークに接続する際、前記遠隔端末から指定された接続先識別符号に基づいて、接続先すべき接続先ネットワークに対応するＩＰネットワーク用網終端装置を特定することを特徴とする。

【００１０】この発明では、ＩＰネットワーク上に配設され、前記遠隔端末が公衆回線網を介してもしくは直接接続されるＩＰネットワーク遠隔接続制御手段により、前記遠隔端末側から指定される接続先に対応するＩＰネットワーク網終端装置との間で送受信するユーザデータをカプセル化することで、仮想専用トンネルを構築する。したがって、物理網を意識せず、またセキュリティを確保してデータの送受信を行うことが可能となる。

【００１１】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

Ａ．実施形態の構成

図１は、本発明の実施形態による全体のシステム構成を示すブロック図である。なお、図５に対応する部分には同一の符号を付けて説明を省略する。図１において、ＩＰネットワーク遠隔接続制御装置１８は、遠隔端末１０１－１、１０１－２側からの接続先の指定に従って、ユーザ＆ＩＳＰネットワーク１０３－１、１０３－２のどちらに仮想専用トンネル１００２－１、１００２－２を構築してデータを振り分けるかの制御を行う。また、ＩＰネットワーク遠隔接続制御装置１８は、上記仮想専用トンネルにデータを送信するためにユーザデータをカプセル化し、ＩＰネットワーク網終端装置１９－１、１９－２との間でＩＰパケット通信を行う。

【００１２】ＩＰネットワーク網終端装置１９－１、１９－２は、ユーザ＆ＩＳＰネットワーク１０３－１、１０３－２のＩＳＰネットワークに接続するためのＩＰネットワークの仮想専用トンネルの閉域網終端装置である。ＩＰネットワーク網終端装置１９－１、１９－２は、仮想専用トンネル１００２－１および仮想専用トンネル１００２－２との経路を接続するインタフェースを有しており、ＩＰネットワーク遠隔接続制御装置１８との仮想専用トンネル（閉域網）を構築後、受信したデータを、ユーザ＆ＩＳＰネットワーク１０３－１または１０３－２に送信する。その際、ＩＰネットワーク網終端装置１９－１、１９－２は、上記ＩＰネットワーク遠隔接続制御装置１８によりカプセル化されたデータからカプセルヘッダを取り除き、ＩＰパケットとしてユーザ＆ＩＳＰネットワーク１０３－１、１０３－２に送信する。



【００１３】エンドユーザの遠隔端末１０１－１は、電話網１００１を介して、遠隔端末１０１－２は、専用線１００３によりＩＰネットワーク遠隔接続制御装置１８と接続されている。遠隔端末１０１－１、１０１－２は、各々、ユーザ＆ＩＳＰネットワーク１０３－１、１０３－１とセキュリティを確保してデータ通信するように、ＩＰネットワーク遠隔接続制御装置１８とＩＰネットワーク網終端装置１９－１、１９－２との間を制御する。

【００１４】次に、図２は、ＩＰネットワーク遠隔接続制御装置１８の構成を示すブロック図である。図２において、ＩＰネットワーク遠隔接続制御装置１８は、接続先振分け機能モジュール２１とカプセル化機能モジュール２２とを備えている。接続先振分け機能モジュール２１は、電話網および専用線を通して受信されたデータをユーザ＆ＩＳＰネットワーク１０３－１、１０３－１のどちらに接続して送信するかを制御する。該接続先振分け機能モジュール２１は、図３（ａ）に示す接続先経路選定テーブル２１０を有している。

【００１５】上記接続先振分け機能モジュール２１は、ユーザの遠隔端末１０１－１、１０１－２側によって指定され、送信されてきた接続先符号を判別し、接続先経路選定テーブル２１０に格納されている、ＩＳＰ識別符号に対応付けられている、仮想専用トンネルの出口となるＩＰネットワーク網終端装置１９－１か、ＩＰネットワーク網終端装置１９－２のいずれかのＩＰアドレスを選択し、仮想専用トンネル１００２－１か仮想専用トンネル１００２－２の経路設定を行う。なお、上記接続先経路選定テーブル２１０は複数設定可能である。

【００１６】カプセル化機能モジュール２２は、上記接続先振分け機能モジュール２１により経路設定された仮想専用トンネルにデータを送信するためにユーザデータをカプセル化する。カプセル化されたユーザデータは、図３（ｂ）に示すフレーム構成を有するＩＰパケットデータ２２０として送信される。該カプセル化機能モジュール２２は、上記ＩＰパケットデータ２２０を、ＩＰネットワーク遠隔接続制御装置１８と、ＩＰネットワーク網終端装置１９－１、１９－２との間をトンネルさせ、ＩＰパケット通信を行う。このとき、カプセル化されたデータ、すなわちＩＰパケットデータ２２０は、ＩＰパケットとして送信されるため、物理網の制約を受けずに通信できる。

【００１７】Ｂ．実施形態の動作

次に、本実施形態の全体の動作について詳細に説明する。接続先振分け機能モジュール２１では、ユーザの遠隔端末１０１－１、１０１－２側によって指定され、送信された接続先符号を判別し、接続先経路選定テーブル

5

２１０を参照し、ＩＳＰ識別符号に対応するトンネルの出口のＩＰアドレスを選択し、該ＩＰアドレスのＩＰネットワーク網終端装置（１９－１または１９－２）に対する仮想専用トンネル（１００２－１または１００２－２）の経路設定を行う。

【００１８】カプセル化機能モジュール２２は、上記接続先振分け機能モジュール２１により経路設定された仮想専用トンネル（１００２－１または１００２－２）にデータを送信するためにユーザデータをカプセル化し、ＩＰネットワーク遠隔接続制御装置１８と、ＩＰネットワーク網終端装置１９－１、１９－２との間でＩＰパケット通信を行う。

【００１９】ＩＰネットワーク網終端装置１９－１、１９－２では、ＩＰネットワーク遠隔接続制御装置１８との仮想専用トンネル（閉域網）を構築後、受信したデータを、ユーザ＆ＩＳＰネットワーク１０３－１または１０３－２に送信する。このとき、図３（ｂ）に示すカプセルヘッダを取り除き、ＩＰパケットとしてユーザデータを送信する。

【００２０】上述した実施形態では、遠隔端末１０１－１、１０１－２からユーザ主導で接続先のユーザ＆ＩＳＰネットワーク１０３－１、１０３－２を選択することができ、接続後、ＩＰパケットをカプセル化するトンネル技術を用いることのみで、物理網を意識せず、またセキュリティを確保してデータの送受信を行うことができる。

【００２１】Ｃ．他の実施形態

次に、本発明の他の実施形態について説明する。図４は、本発明の他の実施形による、複数のユーザ＆ＩＳＰネットワークにＩＰネットワーク経由で接続する際のシステム構成を示すブロック図である。なお、図１に対応する部分には同一の符号を付けて説明を省略する。ＩＰネットワーク網終端装置１９－１～１９－ｎは、各々、対応するユーザ＆ＩＳＰネットワーク１０３－１～１０３－ｎに接続されている。

【００２２】また、ＩＰネットワーク遠隔接続制御装置２８は、図１に示すＩＰネットワーク遠隔接続制御装置１８に相当し、ユーザ＆ＩＳＰネットワーク１０３－１～１０３－ｎの接続先符号と、仮想専用トンネルの出口となるＩＰネットワーク網終端装置１９－１～１９－ｎのＩＰアドレスとが対応付けられた接続先経路選定テーブル（図示略）を備えている。

【００２３】これにより、複数のユーザ＆ＩＳＰネットワーク１０３－１～１０３－ｎにユーザの遠隔端末１０１－１～１０１－ｎ側で指定された複数のユーザ＆ＩＳＰネットワーク１０３－１～１０３－ｎのいずれかに対応する、仮想専用トンネル（閉域網：１００２－１～１００２－ｎのいずれか）を構築し、セキュリティを確保してＩＰパケット通信を行う。

【００２４】なお、上述した閉域網は、論理的な仮想専用線網であるが、この上に物理的な専用線、フレームリレー、ＡＴＭ等の回線を使用した閉域網を重ね、ＩＰネットワーク遠隔接続制御装置１８（または２８）とＩＰネットワーク網終端装置１９－１、１９－２（または１９－１～１９－ｎ）との間を接続して構築した場合でも同様に閉域網を実現できる。

6

【００２５】また、ＩＰネットワーク遠隔接続制御装置１８（または２８）の機能は、図示しない記憶部に記憶されたプログラムを実行することで実現するようにしてもよい。この場合、記憶部は、ハードディスク装置や光磁気ディスク装置、フラッシュメモリ等の不揮発性メモリやＲＡＭ（Random Access Memory）のような揮発性のメモリ、あるいはこれらの組み合わせにより構成されるものとする。また、上記記憶部とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含む。

【００２６】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワークや電話回線等の通信回線のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、上述した処理の一部を実現するためのものであってもよい。さらに、上述した処理をＩＰネットワーク遠隔接続制御装置１８（または２８）に既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

【００２７】以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成は、上記実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【００２８】

【発明の効果】以上説明したように、本発明によれば、ＩＰパケットをカプセル化させるトンネル技術のみでＩＰネットワーク内に仮想専用線網（閉域網）が構築でき、外部からの攻撃に対してセキュリティを確保した通信ができるという利点が得られる。また、これにより、不正侵入を防止するゲートウェイ装置の導入や暗号化等の仕組みの導入が不要となり、設備コストを削減することができ、コストメリットを図ることができるという利点が得られる。

【図面の簡単な説明】

【図１】　本発明の実施形態による全体のシステム構成を示すブロック図である。

【図２】　ＩＰネットワーク遠隔接続制御装置の構成を示すブロック図である。

7

【図３】　接続先経路選定テーブルの構成、およびカプセル化されたユーザデータ（ＩＰパケットデータ）のパケット構成を示す概念図である。

【図４】　本発明の他の実施形による、複数のユーザ＆ＩＳＰネットワークにＩＰネットワーク経由で接続する際のシステム構成を示すブロック図である。

【図５】　従来のシステム構成を示すブロック図である。

【符号の説明】

１８，２８　ＩＰネットワーク遠隔接続制御装置（ＩＰ＊ネットワーク遠隔接続制御手段）

８

１９－１～１９－ｎ　ＩＰネットワーク網終端装置（ＩＰネットワーク網終端手段）

２１　接続先振分け機能モジュール（接続先振分け手段）

２２　カプセル化機能モジュール（カプセル化手段）

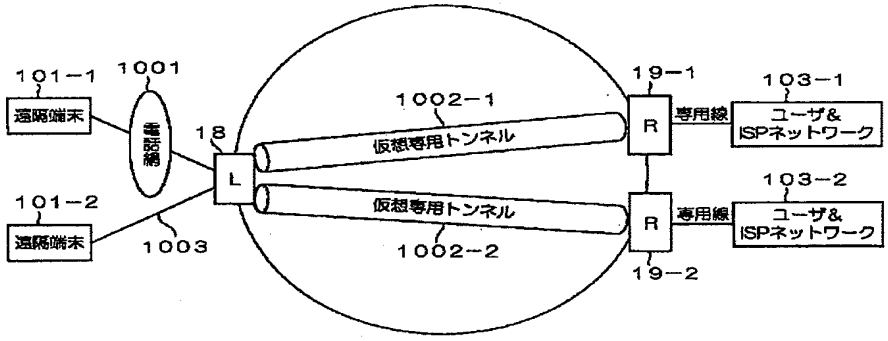
１０１－１～１０１－ｎ　遠隔端末

１０３－１～１０３－ｎ　ユーザ＆ＩＳＰネットワーク

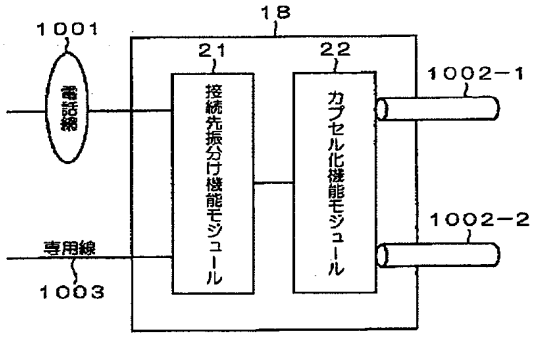
２１０　接続先経路選定テーブル

１００１　電話網

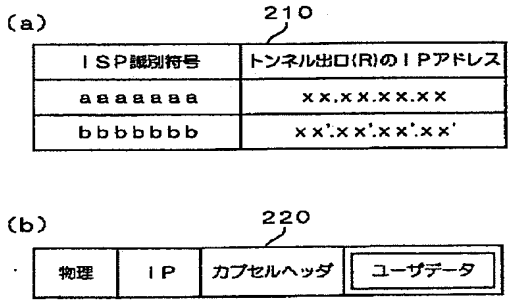
【図Ｉ】



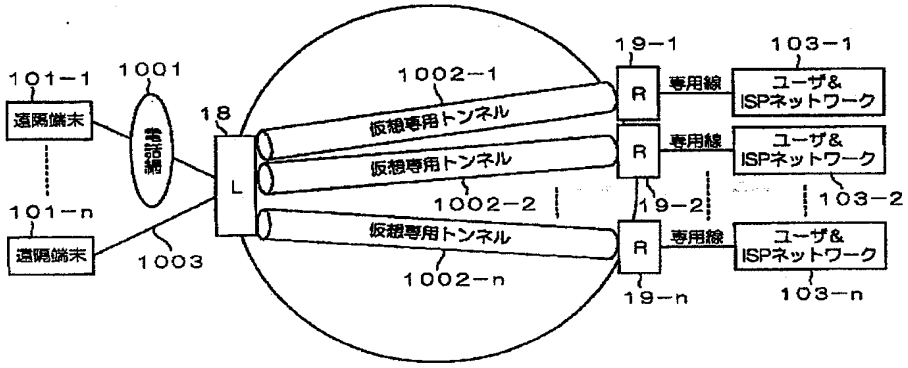

【図２】



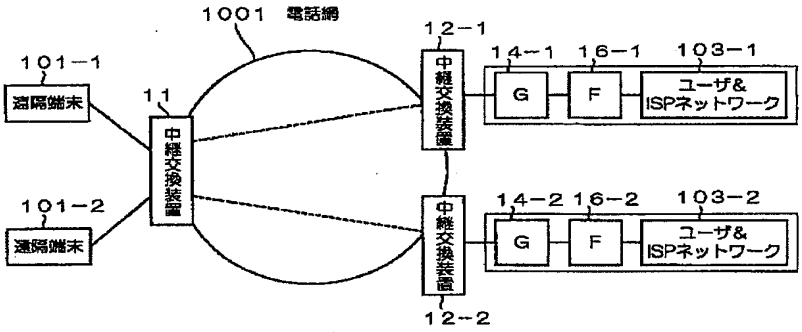

【図３】



【図４】




【図５】




フロントページの続き

(72)発明者　岩渕　光男
東京都新宿区西新宿三丁目19番２号　東日本電信電話株式会社内

Ｆターム(参考)　5K030 GA01 GA15 HA08 HB14 HC02
HD09 JA05 JA08 JL07 KA13
LB02 LE11
5K034 AA02 AA05 BB06 CC01 DD03
EE12 FF09 HH04 HH05 HH07
HH16 HH63 LL01 MM11 NN04